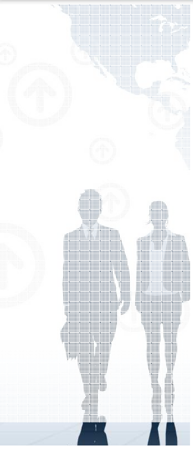
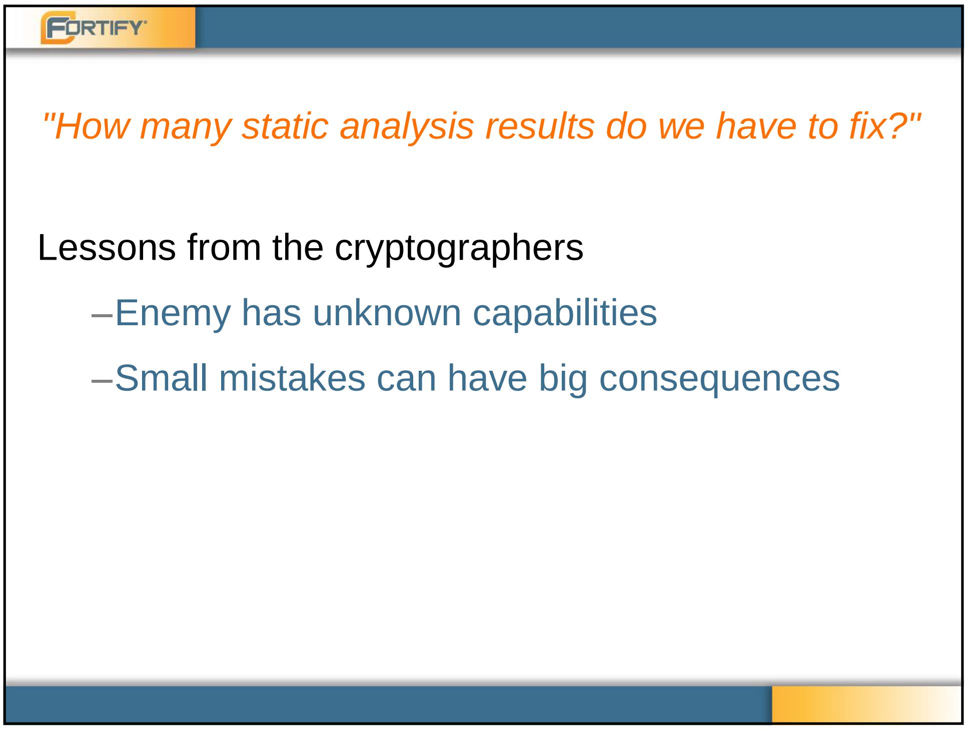


Measuring Software Security Assurance Initiatives

Brian Chess / March 10, 2010

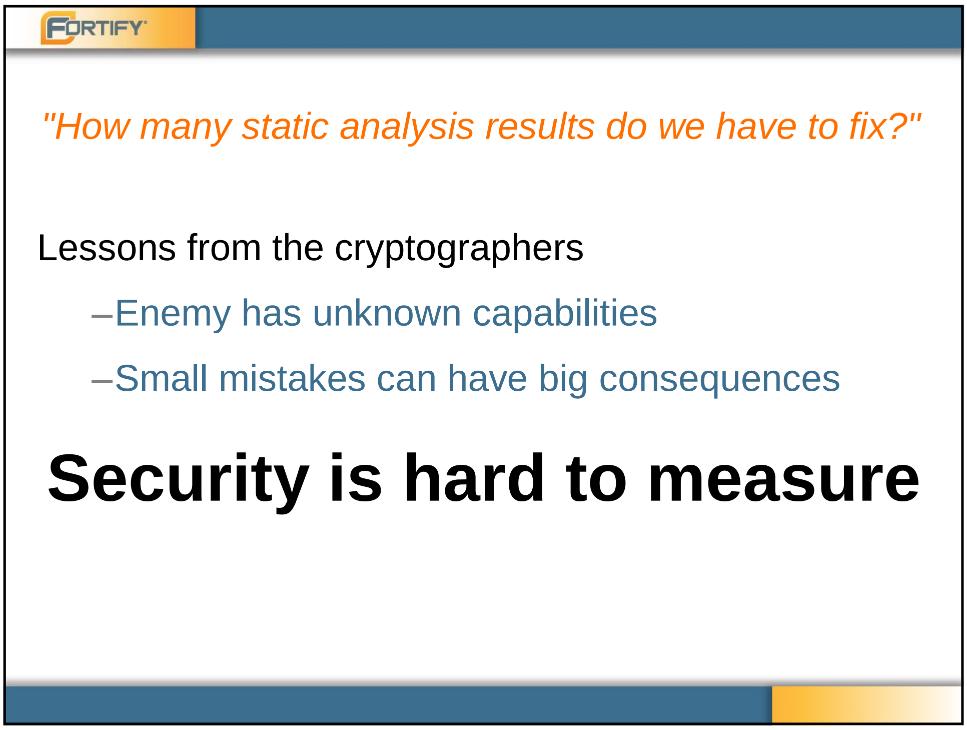
"How many static analysis results do we have to fix?"



"How many static analysis results do we have to fix?"

Lessons from the cryptographers

- –Enemy has unknown capabilities
- –Small mistakes can have big consequences

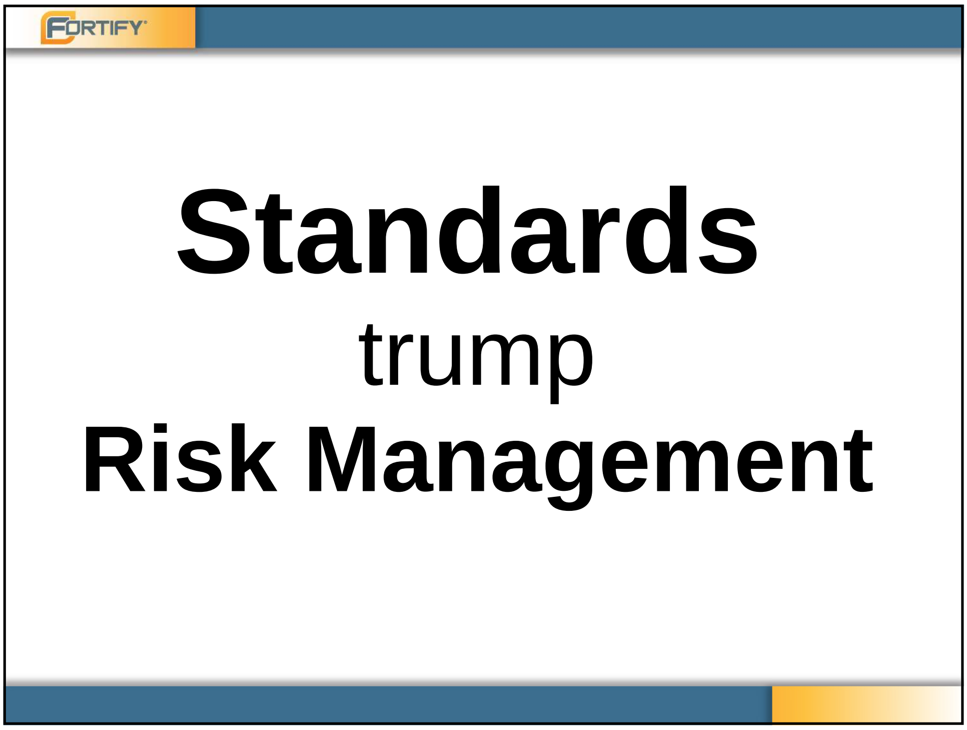


"How many static analysis results do we have to fix?"

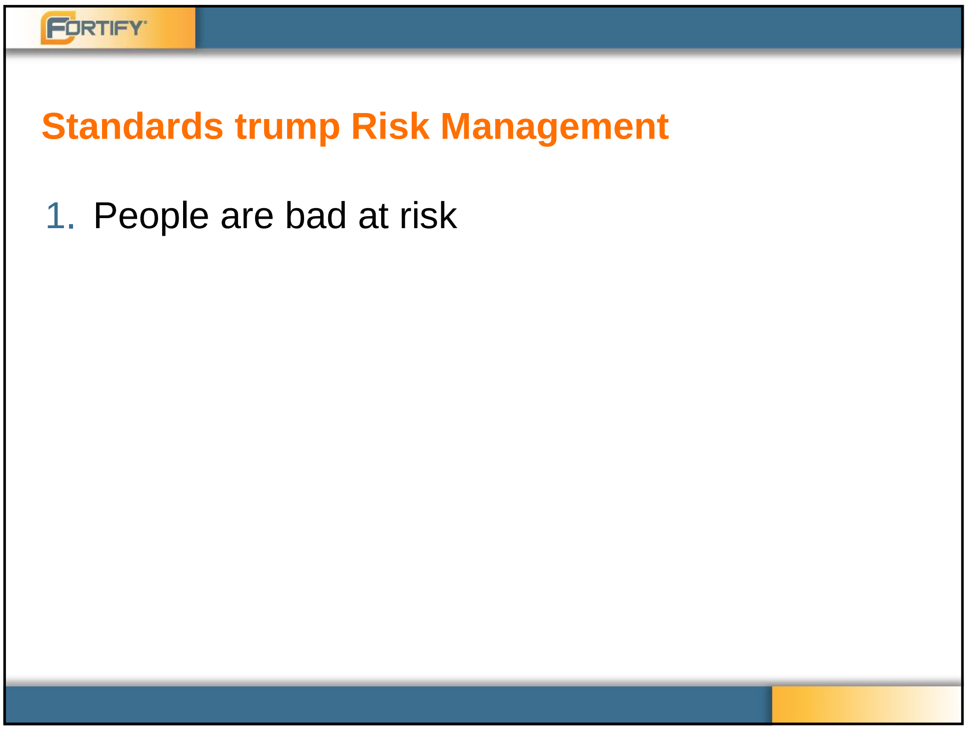
Lessons from the cryptographers

- –Enemy has unknown capabilities
- –Small mistakes can have big consequences

Security is hard to measure



Standards
trump
Risk Management



Standards trump Risk Management

1. People are bad at risk

Standards trump Risk Management

1. People are bad at risk
2. That's not always a bad thing

Transportation
Security
Administration

AIG

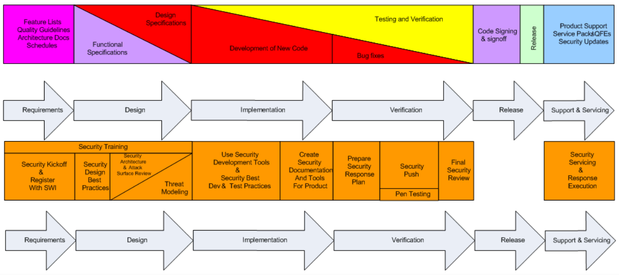
Transportation
Security
Administration

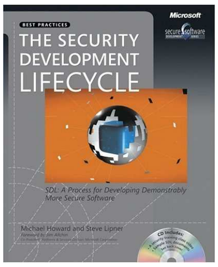
Standards

trump

Risk Management

Security in the Development Lifecycle



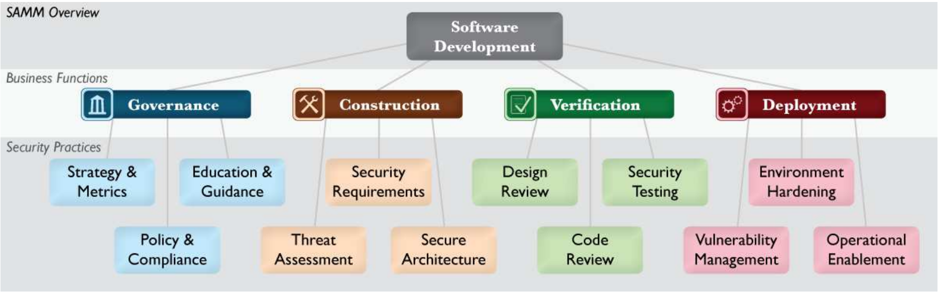

Microsoft
secure software
BEST PRACTICES
THE SECURITY DEVELOPMENT LIFECYCLE
SDL: A Process for Developing Demonstrably More Secure Software
Michael Howard and Steve Lipner
CD Includes:

Initiative > Lifecycle

Creating a software security initiative

- Software Assurance Maturity Model (SAMM)
- Cookbook for security initiatives
- Community-oriented (OWASP)
- http://www.opensamm.org

- Building Security In Maturity Model (BSIMM)
- Real data from real initiatives
- McGraw, Chess, & Migues
- http://bsi-mm.com



SAMM Overview

Software Development

Business Functions

Governance

Construction

Verification

Deployment

Security Practices

Strategy & Metrics

Education & Guidance

Policy & Compliance

Security Requirements

Threat Assessment

Secure Architecture

Design Review

Security Testing

Code Review

Environment Hardening

Vulnerability Management

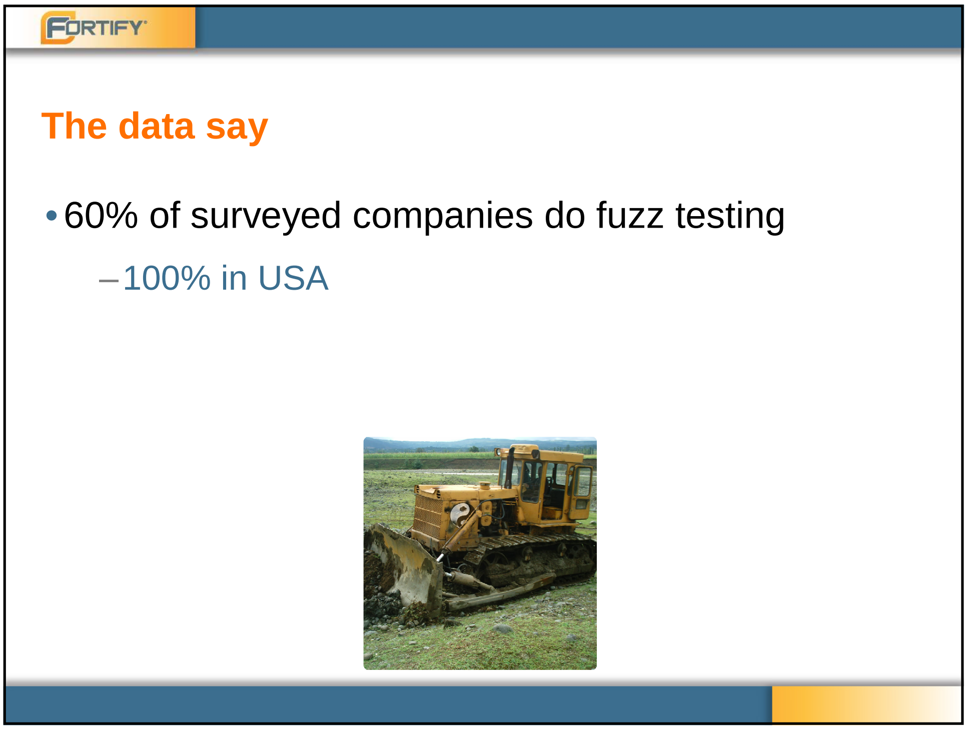
Operational Enablement

One framework for describing all software security assurance initiatives.

Data
are good

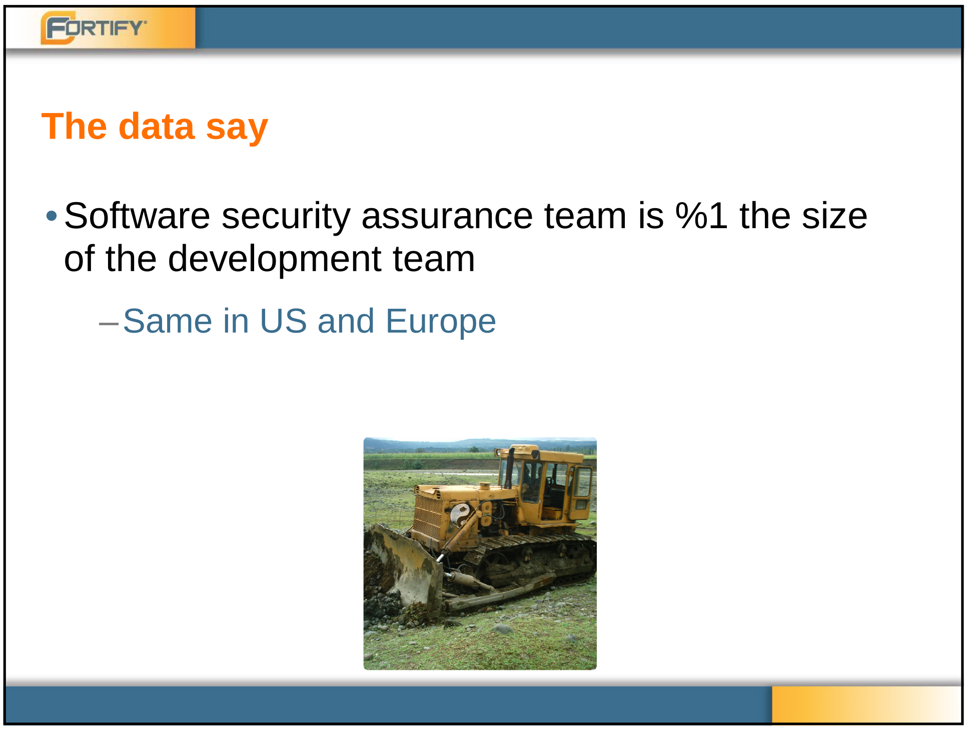
The data say

- 67% of surveyed companies use static analysis
  - 88% in USA



The data say

- 60% of surveyed companies do fuzz testing
  - –100% in USA



The data say

- Software security assurance team is %1 the size of the development team
  - –Same in US and Europe

The data say

- Training hollow

The data say

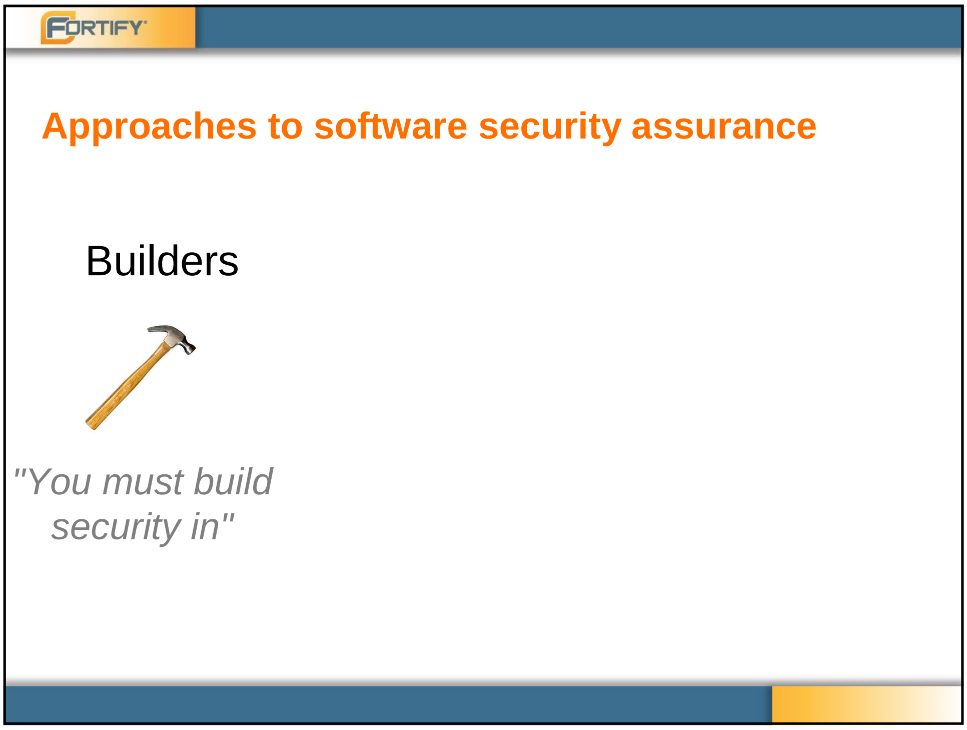
- Banks do compliance better than ISVs

The data say

- Little flow between verification tools

The data say

- Resources split between governance, construction, verification, and response



Approaches to software security assurance

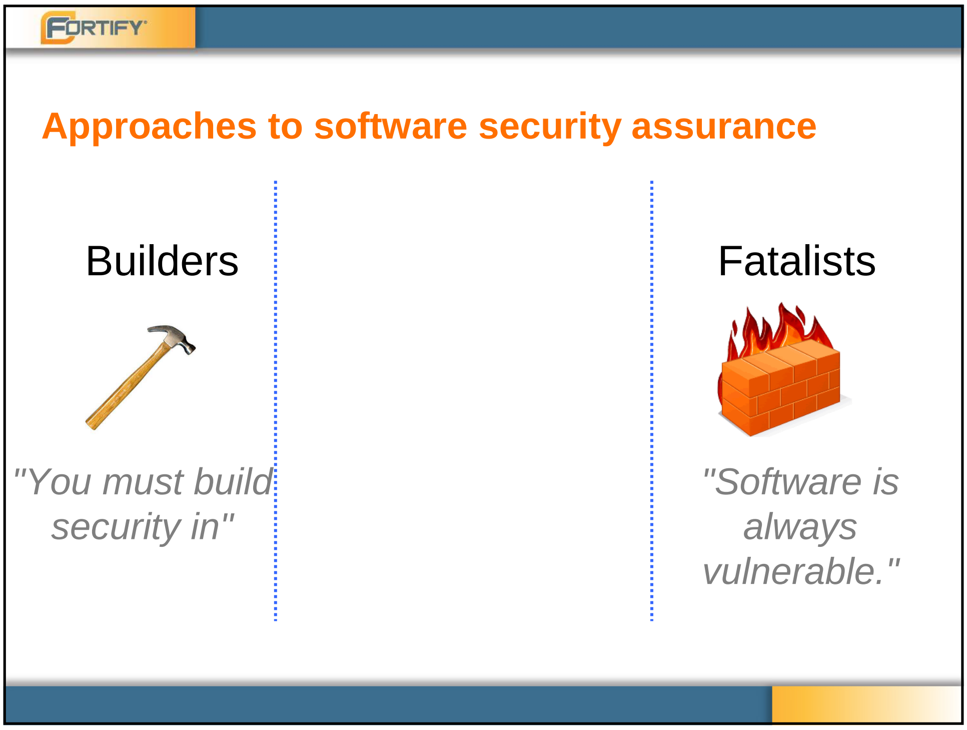
Builders

"You must build security in"

Approaches to software security assurance

Fatalists

"Software is always vulnerable."



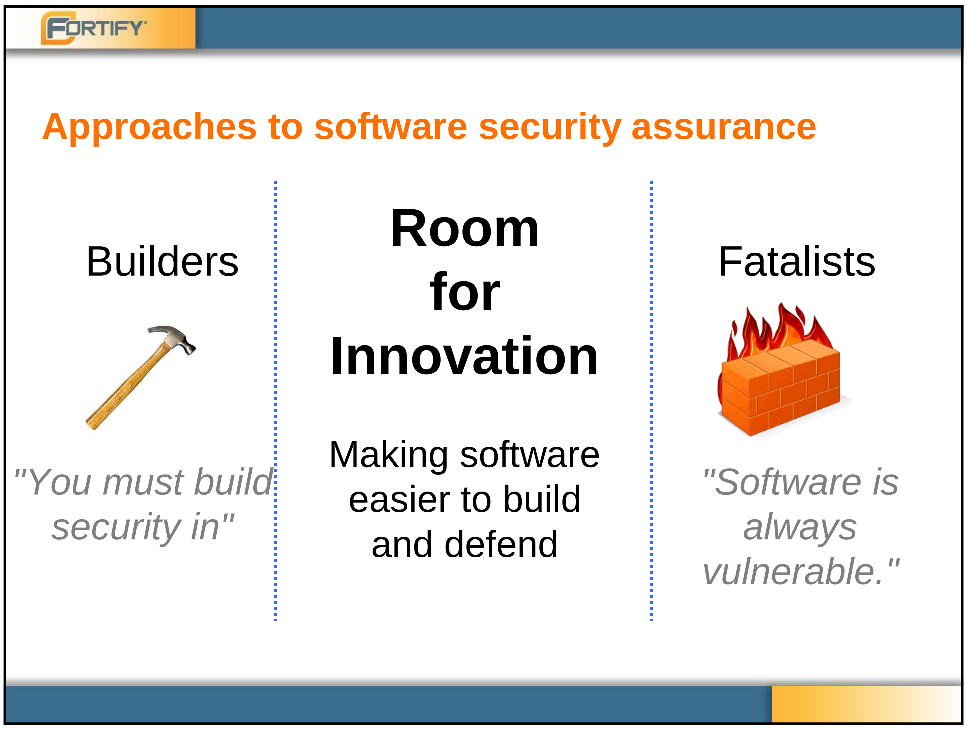
Approaches to software security assurance

Builders

"You must build security in"

Fatalists

"Software is always vulnerable."



Approaches to software security assurance

Builders

"You must build security in"

Room for Innovation

Making software easier to build and defend

Fatalists

"Software is always vulnerable."

Conclusion

- Invest in standards
- Measure process
- Blend construction and reaction